# 1.13 Mission Assurance Modeling and Simulation: A Cyber Security Roadmap

## Mission Assurance Modeling and Simulation: A Cyber Security Roadmap

Gerald "Jay" Gendron
*gerald.gendron@gmail.com*

David Roberts
Donold Poole, CISSP
Anna Aquino
SimIS Inc.
Portsmouth, VA 23704
*{david.roberts, donold.poole, anna.aquino} @simisinc.com*

**Abstract**. This paper proposes a cyber security modeling and simulation roadmap to enhance mission assurance governance and establish risk reduction processes within constrained budgets. The term mission assurance stems from risk management work by Carnegie Mellon's Software Engineering Institute in the late 1990s. By 2010, the Defense Information Systems Agency revised its cyber strategy and established the Program Executive Officer-Mission Assurance. This highlights a shift from simply protecting data to balancing risk and begins a necessary dialogue to establish a cyber security roadmap. The Military Operations Research Society has recommended a cyber community of practice, recognizing there are too few professionals having both cyber and analytic experience. The authors characterize the limited body of knowledge in this symbiotic relationship. This paper identifies operational and research requirements for mission assurance M&S supporting defense and homeland security. M&S techniques are needed for enterprise oversight of cyber investments, test and evaluation, policy, training, and analysis.

### 1.0 INTRODUCTION

> *It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity…*
>
> ~Charles Dickens

This opening passage from Charles Dickens' 1859 classic *A Tale of Two Cities* seems a fitting statement of cyber space in the early twenty-first century. How timeless Dickens' sense of blessings and curses – and applicable to the modern-day Information Age. This sense of paradox motivated the authors to consider the topic of cyber security and launch a discussion about the balance that must be established in the realm of cyber operations. The objective is to blaze a trail towards a Cyber Security Roadmap, specifically a roadmap harnessing the talents of both operators and operations analysts in a collaborative partnership and develop concrete actions which address these questions: how can models and simulations add value to cyber security as they have with test and evaluation, design, and decision making?

The term *mission assurance* was found in the literature as early as the early 1990s out of Carnegie Mellon's Software Engineering Institute. Their seminal work in this area used the term within the context of risk management. In the estimation of the authors, this approach leaning on risk management is a timeless rendering of the term mission assurance and is noted here for its sound approach. Unfortunately, within the context of information assurance, risk management is often misinterpreted as risk *avoidance.* Highlighting the importance of word choice, the Defense Information Systems Agency revised its cyber strategy. As part of reorganization, the Agency established the office of the Program Executive Officer – Mission Assurance.

The authors envision a Cyber Security Roadmap which addresses two key characteristics. The first is governance.

> **How can cyber security policies and practices be established to best articulate operational requirements which could benefit from analytical collaboration?**

Second is the treatment of risk management.

> **What actions can facilitate a shift in information assurance culture to best integrate the treatment of risk management into the enterprise?**

For instance, the National Institute of Standards and Technology (NIST) Special Publication 800-39 entitled "Integrated Enterprise-Wide Risk Management" is a recent, cutting-edge work dedicated to shifting the culture with regard to better understanding the proper tenets of risk management [1].

## 2.0 LITERATURE REVIEW

The concept of mission assurance is emerging as a shift in culture and perspective from information assurance. Mission assurance provided the authors with a compelling vision of the need for further research in this area. Their goal was to review the body of unclassified literature for work in the area of modeling and simulation supporting information security. This section summarizes the results of a modest literature review using sources from both academia and industry.

The methodology used to research the academic body of knowledge was by means of the EBSCOhost search engine made available through National Defense University in Washington, D.C. Less than a dozen references were identified which met the Boolean search parameters for both "modeling and simulation" as well as "information security". Many of the resultant articles were related to the simulation of cryptologic key algorithms and not directly applicable to this paper. These scant results led the authors to carefully consider their search techniques to ensure a body of work was not being overlooked. Results could not be improved by using variations on the search terms. It was later learned in researching open source commercial work that the field of modeling and simulation in support of information security is either fairly nascent or classified.

Three peer-reviewed journal articles were most interesting in their treatment of analysis within cyber security. Sahinoglu [2] presents his work on the need for quantitative methods to improve risk management techniques in software intensive systems. He presents a Security Meter Model based on a relatively classic representation of risk:

$$RR = \text{Vulnerability} \times \text{Threat} \times \text{LCM} \quad (1)$$

where RR is the Residual Risk and LCM represents a Lack of Countermeasure. Using Bayesian probability methods, Sahinoglu [2] determines the probability data for various threats pertaining to sets of vulnerabilities. His objective is to quantify enhanced risk postures relative to the incremental costs of countermeasures, "guiding the security manager as to how one can move to a more advantageous state from the present" ([2], p. 1257). In essence, Sahinoglu's work establishes an objective and quantitative cost-benefit approach to capital planning of information security investments.

An article by Kumar, Park, and Subramaniam [3] entitled "Understanding the Value of Countermeasure Portfolios in Information Security Systems" presents an analysis which complements the work by Sahinoglu. Their work focuses on the

challenges organizations face to properly "understand the economic consequences of security attacks relative to the ISSC [information system security countermeasures] portfolio implemented" ([3], p. 241). Kumar, Park, and Subramaniam make three key contributions to the body of literature:

- developing a simulation to integrate threat, prevention, and recovery;
- investigating how to better model interactions among business, threat, and countermeasure parameters;
- recognizing an information security portfolio is dynamic and discusses models and simulations based on financial asset valuation.

Kumar, Park, and Subramaniam [3] – like Sahinoglu [2] – offer knowledge for potential use in a Cyber Security Roadmap. Finally, an article by Ying, Lin. Lee, and Lin [4] investigates some sophisticated modeling based on neural networks to classify an increasing threat in today's cyber environment – unwanted emails. It focuses on filtering spam e-mail. Their work can be used more generally to model the identification of other types of unwanted e-mail such as the increasing difficulties in interdicting e-mails used to perpetrate spear-phishing attacks.

In addition to more traditional sources from academia, the Google search engine provided the authors with a glimpse into industry's body of knowledge with regard to modeling and simulation in support of information security. Due to the author's desire to maintain research at the unclassified level, the results of the literature review were relatively meager. This could be due to limited work in this field, lack of transparency in the interest of closely held corporate research, or the potentially classified nature of this work. However, there were two professional forums that have had recent professional events including industry members that pierced the subject of interest. Most notably was the conference held in March 2011 under the auspices of the Military Operations Research Society entitled "Mission Assurance: Analysis for Cyber Operations" [5]. This special meeting was a follow up event to a 2008 Cyber Analysis Workshop held in Reston, Virginia [6]. Additionally, a second forum of note was the 16th International Command and Control Research and Technology Symposium held in June 2011 by the Command and Control Research Program out of the Office of the Assistant Secretary of Defense (NII). In particular, a Cyber track was added to this year's Symposium and highlighted the need for future research in this area.

## 3.0 "GAME CHANGERS" FOR CYBER ANALYSIS

This section provides a summary of the two events to include event objectives, key findings, and recommendations. These events publically identified a need to develop solutions for problems associated with analysis of cyber security.

### 3.1 Military Operations Research Society Special Meeting

The Military Operations Research Society (MORS) is a professional organization dedicated to understanding the needs of military users and encourages operations research to support military operations [7]. When particularly broad-reaching and complex operational problems emerge within the defense sector, MORS has sometimes called for a Special Meeting on the subject to bring together experts from academia, industry, and the government to begin a dialogue on the issue. In March 2011, conditions warranted the establishment of a Special Meeting entitled "Mission Assurance: Analysis for Cyber

Operations". From March 21 – 24, 2011, a diverse body of people including operational analysts and information technology specialists convened at Southwest Research Institute in San Antonio, Texas. Their express purpose was to establish cross-functional working groups to consider four primary components of cyber security: (a) situational awareness; (b) establishing and extending networks; (c) operating and defending networks; and (d) the application of cyber force. The Special Meeting had four objectives:

- Enhance understanding of cyber threat among participants;
- Advance analytical methods to support cyber operations;
- Facilitate conversation among operators, analysts, and cyber customers to improve mission assurance;
- Write an unclassified report with classified appendices articulating analytic techniques and posit recommendations to improve cyber operations and mission assurance [6].

The four working groups generated many findings and recommendations which are too numerous to completely discuss in this paper. The authors encourage interested readers to visit the MORS website [6] to access and read the Special Meeting agenda, working group presentations and the final briefing synthesized from those working groups. The authors would like to highlight a few key findings and their associated recommendations as they relate to Mission Assurance Modeling and Simulation and a Cyber Security Roadmap. First among these are findings related to operationally define and communicate the problems [5]. Terms like Mission Assurance and Cyber Domain must be defined among various functional groups from operators to analysts. Likewise, consistent lexicon and metrics currently do not exist to forge discussions among operational and analytical professionals. MORS recommendations include:

- establishing tactics, techniques, and procedures as well as doctrine;
- refining and using a "Joint Staff Cyber Lexicon" ([5], slide 17);
- articulating cyber networks, attacks, and defenses in operational planning terms and the Joint Operation Planning Process.

Secondly, many operational support-oriented findings were presented ranging from training to organizing and equipping operational forces. Most notable among the findings was the lack of mutual understanding between cyber operators and the analytic community – the former discuss the problem in qualitative terms whereas the latter desire direct metrics. Cyber operators typically lack knowledge of how operational analysis can assist operations and the analytic community currently has few practitioners interested in cyber warfare. Additionally, cyber warfare is in the nascent stage of development without an organized body of knowledge and subject to inadequate or inefficient practices, organizational constructs, and policies. MORS recommendations include:

- establishing a MORS Cyber Analysis Community of Practice;
- nurturing more work in the area of cyber analysis;
- communicating how analysis could aid the cyber operations force.

This is as much a matter of emphasis and leadership as it may be related to funding and training.

Finally, there are future research areas articulated in the MORS findings and recommendations. Numerous operations

research techniques such as Statistical Process Control, Design of Experiments, Neural Networks, optimization methods, and Decision Analysis tools can be employed to model and analyze the networks themselves as well as cyber enablers like manpower and portfolio prioritization. The forum also found an unsatisfactory understanding of cyber and virtual threats. MORS recommendations include:

- developing force-on-force models that account for cyber effects and activities;
- building a bibliography of existing literature on this area;
- establishing more rigorous analysis of the threat;
- highlighting the need for leadership in this area to make this a priority across the Services and instilling a *pull* from the cyber force.

### 3.2 Command and Control Research Program Symposium

The Command and Control Research Program (CCRP) is a group within the Office of the Assistant Secretary of Defense (NII) dedicated to improve the state of command and control while increasing the understanding of implications of the Information Age on national security [8]. Additionally, it sponsors an annual symposium called the International Command and Control Research and Technology Symposium (ICCRTS). From June 21-23, 2011, the 16th ICCRTS convened in Québec City, Québec. Participants from over 20 countries included members of academia, industry, and government. This symposium marked the addition of a new track on Cyberspace Management. Proceedings from this event are available online [9]. Presentations for this track were diverse in focus and very professional. There was also ample discussion on how this track may and should evolve. The track chair noted a desire for papers in next year's event addressing foundational elements of this subject area such as terms of reference, understanding differences between cyber domains and functions, and identifying research needs in the cyber arena.

In addition to this new track, the CCRP Director, Dr. David Alberts, presented summary findings of a draft paper stemming from CCRP workgroup SAS-065 on the NATO NEC C2 Maturity Model. The goal of workgroup SAS-065 was "to create a NATO NEC C2 Maturity Model (N2C2M2) to facilitate the exploration of network-enabled command and control approaches and capabilities in a coalition context" ([10], p. 1). The N2C2M2 includes metrics to help organizations assess their capabilities relative to command and control. SAS-065 was formed in 2006 before the emergence of US Cyber Command. Nonetheless, additional research is indicative of the agility of this model for contemporary issues like cyber security. Noteworthy of the Alberts presentation as it relates to the subject of this paper are his findings that cyber can and should be analyzed in further detail.

## 4.0 CYBER SECURITY ROADMAP

Based on information in the literature review, the authors propose that the operational and analytic community may best be served through their collaboration in developing and concurring on a Cyber Security Roadmap. This paper proposes a broadly defined Roadmap as a first enumeration of a more detailed and necessary one to be developed in the near term. Its primary objective is to stimulate discussion and collaboration among the various communities of interest which impact or are impacted by cyber security issues. This first cut certainly does not get everything right, but it serves as progress towards a practical end. This initial roadmap touches on two key elements:

operational requirements and research requirements. It currently does not address a third important element which is the temporal aspects of a more refined Roadmap. This is important to help drive decision and funding cycles of the operational and research requirements. Temporal aspects are best addressed by a collaborative team of stakeholders.

## 4.1 Operational Requirements

United States Cyber Command has the mission to develop and staff issues related to the war fighting functions of offensive and defensive cyber operations. In addition to cyber operations, there are four broad areas of operational support where a Cyber Security Roadmap could offer tangible, strategic end states to guide the operational and analytic communities:

- Cyber Policy
- Investment Strategy
- Test and Evaluation
- Training Development

Briefly touching on each area, *policy makers* may benefit from modeling and simulation to forecast and evaluate policy frameworks against various operational environments and national strategies. This could provide insights as to the impact of various policy measures on cyber operations. Likewise, alternative *investment strategies* could be investigated through modeling and simulation to identify gaps and seams in cyber security portfolios with respect to threats, vulnerabilities, and countermeasures.

The *test and evaluation* community has long relied on the capabilities inherent in modeling and simulation to accomplish assessments more effectively under constrained resources. A Cyber Security Roadmap should articulate a vision of effectively conducting test and evaluation on weapon systems as cyber operations become more mature. For instance, what does cyberspace *look like?* Perhaps we should embark on an era of great explorers like Vespucci and Columbus. These Renaissance men were explorers, navigators, and cartographers – making the unknown world visible though mapping. Modern-day explorers could define the landscape of cyber space to the benefit of the test and evaluation community. Finally, *training* operators about cyber and with cyber will require a cyber approach. Modeling and simulation should be considered more widely to augment live cyber training events. Not only can simulations generate synthetic training environments, they can be used to collect data to better quantify training effectiveness.

## 4.2 Research Requirements

In addition to enablers to cyber operations, there are subjects requiring further research with respect to cyber security. The authors have identified three broad areas to categorize research elements of a Cyber Security Roadmap:

- Analytic Capabilities
- Test Infrastructure
- Risk Reduction

### 4.2.1 Analytic Capabilities

This paper advocates the need for baseline models and simulations for use among partners investigating and analyzing cyber security topics. Potential actions include:

- Capture the current knowledge relevant to the modeling and simulation of information security vulnerabilities and protections, to include incident management. The outcome should identify the needs, translate them into requirements, and provide summary information on resources available to meet the needs and requirements. Since the

landscape of cyber threat environments will be continuously changing, these baseline requirements are intended to be utilized in a suitable systems engineering approach to enable agile and assured systems.

- Decompose the requirements into actionable segments.
- Expand trust-relevant requirements (whether automatically generated or manually specified) beyond control measures described in standards or policy documents.
- Develop trust models and metrics to be used in engineering of system into measurable system attributes and then in testing and assessment.
- Advocate for composable components that could be rapidly reconfigured for addressing unforeseen circumstances.
- Determine ways to treat human behavior representation.
- Prioritize data governance – not all information is original or critical. Channel resources for data protection.
- Determine how to automate threat analysis from several sources to discern cyber attacks and develop remediation strategies.

### 4.2.2 Test Infrastructure

The term *test and evaluation* is a familiar term representing the ability to assess systems for war fighter effectiveness and suitability. A less common thought with respect to test and evaluation is that its execution relies on a harmoniously balanced interplay among diverse partners. The test and evaluation infrastructure arrayed across the globe helps join these partners. It is also one of the great behind-the-scenes aspects of test and evaluation which is commonly misunderstood. The Test Resource Management Center is responsible for development of next generation test infrastructure to support test and evaluation in the coming decades. The Cyber Security Roadmap should articulate what cyber security test requirements are looming in the distance so research and development of the requisite test infrastructure will exist to support acquisition program needs. Potential actions include:

- Research systems engineering approaches. This may include an open systems engineering environment that promotes logical and virtual test designs before physical test designs.
- Shift approaches more closely to the optimal model-evaluate-build concept.
- Conduct pilot evaluations using sufficiently mature technologies to perform exploratory development, advanced development, and support actionable segment(s).

### 4.2.3 Risk Reduction

Risk management concepts are fairly well captured in many bodies of literature. Specifically, the Federal Information Processing Standards publications from the National Institute of Standards and Technology do a very good job of outlining risk management in cyber operations. There exists a need for social research on how well the culture is changing from information assurance to mission assurance. Potential actions include:

- Determining individual and organizational ability to rapidly adapt to unforeseeable threats or opportunities.
- Articulate solution-assurance goals so the resulting systems are trusted, assured, reliable, and interoperable.
- Ability to move from compliance, typically a point-in-time objective, to

continuous monitoring and automated remediation strategy.

## 5.0 CONCLUSION

*It is our choices that show what we truly are, far more than our abilities.*

~J.K. Rowling (Harry Potter)

This paper proposes a cyber security roadmap to enhance mission assurance governance and establish risk reduction processes within constrained budgets. The authors begin with a summary of a literature review in this nascent field of study. They also point out many emerging issues in this area which have gained recent attention by key professional groups. A key first step is to identify collaborative opportunities among cyber operators and operations analysts. Professional societies note these two groups have not been the focus of leadership attention and they could work more closely together. The Military Operations Research Society has gone so far as to recommend establishment of a cyber community of practice.

Finally, this paper presents thoughts and recommendations on two key elements of a Cyber Security Roadmap: operational and research requirements. Operationally, this Roadmap suggests four broad areas to focus discussions and end states: cyber policy, investment strategy, test and evaluation, and training development. Each of these four areas stands to benefit from modeling and simulation to aid decision making. Likewise, this Roadmap suggests three broad areas to focus future research in support of cyber security: analytic capabilities, test infrastructure, and risk reduction. These research areas encompass a holistic approach ranging from analytic techniques to the quest for new test technologies to research on human and cultural impact on the sense of risk.

One key element not addressed in this Cyber Security Roadmap is the temporal aspects. This is important to help drive decision and funding cycles of the operational and research requirements. Temporal aspects are best addressed by a collaborative team of stakeholders.

## 6.0 REFERENCES


[1] National Institute of Standards and Technology (NIST). (2010, December). *Integrated enterprise-wide risk management: Organization, mission, and information, system view* (Special Publication 800-39). Gaithersburg, MD: US Department of Commerce.

[2] Sahinoglu, M. (2008, June). An input-output measurable design for the security meter model to quantify and manage software security risk. *IEEE Transactions on Instrumentation and Measurement, 57 (6), 1251-1260.*

[3] Kumar, R. L., Park, S., & Subramaniam, C. (2008, Fall). Understanding the value of countermeasure portfolios in information security systems. *Journal of Management Information Systems, 25 (2), 241-279.*

[4] Ying, K. C., Lin, S. W., Lee, Z. J., & Lin, Y. T. (2010). An ensemble approach applied to classify spam e-mails. *Expert Systems with Applications, 37, 2197-2201.*

[5] Military Operations Research Society. (2011a, March 24). Synthesis group final report from *Mission Assurance: Analysis for Cyber Operations Conference* [PDF document]. Retrieved from http://www.mors.org/UserFiles/file/2011

%20Cyber%20Assurance/Outbriefs/MORS%20Cyber%202011%20Synthesis%20Final%20Briefing%20(V3).pdf.

[6] Military Operations Research Society. (2011b). *Terms of reference.* Retrieved from http://www.mors.org/UserFiles/file/2011%20Cyber%20Assurance/MORS%20Cyber%202011%20Working%20Group%20TOR%20and%20Agenda%208%20Mar.pdf.

[7] Military Operations Research Society. (n.d.). *MORS goals and code of ethics.* Retrieved from http://www.mors.org/about/code.aspx.

[8] Command and Control Research Program. (n.d.). *About the program.* Retrieved from http://www.dodccrp.org/html4/about_main.html.

[9] International Command and Control Research and Technology Symposium. (n.d.). *Proceedings from 16th international command and control research and technology symposium.* Washington, D.C. Retrieved from http://www.dodccrp.org/events/16th_iccrts_2011/post_conference/html/tracks.html.

[10] NATO SAS-065 Research Task Group. (n.d.). *NATO NEC C2 maturity model.* Retrieved from http://www.dodccrp.org/sas_files/n2c2m2_final_draft.pdf.